Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Communications Assistance for	)	ET Docket No. 04-295
Law Enforcement Act and	)	
Broadband Access and Services	)	RM-10865
	)	

COMMENTS OF FIDUCIANET, INC.

H. Michael Warren
President
Fiducianet, Inc.
mike.warren@fiducianet.biz

Douglass J. McCollum
General Counsel, VP Services
doug.mccollum@fiducianet.biz

2121 Cooperative Way
Suite 200
Herndon, Virginia 20171
Tel: (703) 796-1100
Fax: (703) 689-0566

November 8, 2004

TABLE OF CONTENTS

SUMMARY

Fiducianet is a third-party service provider that offers a full range of services to telecommunications carriers and service providers,[1] including new entrants such as VoIP service providers and traditional Internet service providers (hereinafter jointly and severally referred to as "service providers"). Through their agent, service providers fulfill the burdensome, complex and expensive responsibility of procuring/deploying technical solutions and provisioning the technical assistance required by the Communications Assistance for Law Enforcement Act of 1994 [codified in principal part at 47 U.S.C. §§ 1001 *et seq*. ("CALEA")] or by court orders issued under federal and state electronic surveillance laws in order to make the electronic surveillance operational.

None of Fiducianet's options involves the transmission of intercepted call content or call-identifying information on a network that is separate and apart from the service provider's network. Rather, Fiducianet deploys solutions that reside entirely within the service provider's network so that it is similar to a solution that a service provider itself might deploy using its internal staff.

Once compliant technology has been installed in the service provider's network, tested and provisioned, Fiducianet delivers the call content and/or call-identifying information directly from the service provider's network to a location or facility acceptable to law enforcement and in a format consistent with industry standards.

[1] For the purposes of the comments, "service providers" refers to telecommunications carriers that are subject to CALEA

Fiducianet has invested in state-of-the-art technology to carry out these technical assistance responsibilities. Equally important, it is managed by persons with deep domain knowledge and extensive experience in law enforcement, law enforcement support services operations, and the telecommunications industry. Because of this knowledge and experience, Fiducianet understands the needs and constraints of both the service providers and law enforcement and works with service providers and manufacturers to develop streamlined services that meet the assistance-capability requirements of Section 103(a) of CALEA.

Fiducianet pays close attention to protecting the privacy and security of the service provider's customers. It ensures that the content and/or call-identifying information that the court has authorized to be intercepted, and only this content and/or call-identifying information, is made available to law enforcement from the service provider's network. At the same time, Fiducianet is acutely aware of law enforcement's need for strict compliance with the non-disclosure obligations of the applicable laws as well as the court orders themselves. Fiducianet has its own strict non-disclosure policies, all of its employees execute non-disclosure agreements, its employees undergo background and credit checks, and Fiducianet stores all relevant documents and records under secure arrangements. All of these steps ensure that the existence of the electronic surveillance is not disclosed except as authorized by law.

Fiducianet also uses its proprietary software to respond to subpoenas, court orders and search warrants and to produce the records specified. Its automated systems fulfill subpoenas, court orders and search warrants in a timely, efficient and cost-effective manner, usually within 1 to 3 days.

Fiducianet's end-to-end services offer service providers, manufacturers, and law enforcement an efficient and a cost-effective solution for increasingly demanding and complex law enforcement support service responsibilities.

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Communications Assistance for	)	ET Docket No. 04-295
Law Enforcement Act and	)	
Broadband Access and Services	)	RM-10865
	)	

COMMENTS OF FIDUCIANET, INC.

Fiducianet, Inc. ("Fiducianet") submits these comments in response to the Notice of Proposed Rulemaking ("NPRM") released on August 9, 2004, and published in the Federal Register on September 23, 2004 (69 Fed. Reg. 56976 *et seq*.), and pursuant to applicable Federal Communications Commission ("FCC" or "Commission") Rules.

I. INTRODUCTION

Fiducianet is one of two entities the NPRM designates as a "trusted third party," (NPRM, III.C.2, ¶¶ 69-76), or a "third party CALEA service provider," (*e.g*., ¶ 93), or a "third party provider," (*e.g*., ¶ 103), or mentions by name, (¶ 69 n. 184). The NPRM describes several "third party" solutions in general. Fiducianet's comments will explain in more detail why service providers engage its services, how it provides its services so as

to protect the privacy and security interests of the service providers and their customers, as well as law enforcement, and why the solutions chosen by Fiducianet meet the electronic surveillance needs of law enforcement as well as the requirements prescribed by CALEA and the electronic surveillance laws.

Fiducianet will also comment on several questions raised in the NPRM that relate to its services.

II. BACKGROUND

In reconciling the differing views of law enforcement agencies, service providers, and public interest groups about CALEA and about the role of service providers in electronic surveillance in general, the FCC finds itself in the middle of a long-standing controversy. For years, service providers have attempted to balance the conflicting obligations of protecting the privacy interests of their customers while at the same time fulfilling the lawful and ever-increasing demands of law enforcement for subscriber information and call detail records as well as demands for technical assistance for electronic surveillance.

The origins of these conflicting obligations can be found in Section 605 of The Communications Act of 1934 and the cases interpreting Section 605.[2] With respect to the records created by service providers that contain detailed information about a customer's calling patterns, for example, the court held that Section 605 did not apply to the release

[2] One of the principal services Fiducianet offers to service providers is serving as custodian of records and handling subpoenas, court orders and search warrants for the production of subscriber information and toll or call detail records. After validating and clarifying the subpoena, court order or search warrant, Fiducianet uses its proprietary software to produce the records specified in the lawful process. Because of the efficiencies of its automated systems, Fiducianet is able to respond to criminal subpoenas within 1 to 3 days.

of telephone toll records because they are business accounting records that subscribers know the telephone company prepares in the regular course of its business. *United States v. Costello*, 410 F.2d 536 (2nd Cir. 1969). *Costello* and similar decisions of other courts foreshadowed *Smith v. Maryland*, 442 U.S. 735 (1979), which held that there is no Fourth Amendment protection for toll records created by telephone companies in the regular course of their business. Service providers now respond to well over a million subpoenas, court orders, and search warrants annually for the production of subscriber information and toll or call detail records. Except in very limited circumstances, however, service providers bear entirely the burdensome cost of producing these records for law enforcement. *Hurtado v. United States*, 410 U.S. 578 (1973); s*ee Ameritech v. McCann*, 297 F.3d 582 (7th Cir. 2002).[3]

Title III of The Omnibus Crime Control and Safe Streets Act of 1968, codified, as amended, at 18 U.S.C. §§ 2510 *et seq*., (hereinafter Title III), resolved a long-standing national debate whether law enforcement could engage in electronic surveillance and whether the results of such surveillances would be admissible in court. Telephone companies, however, resisted voluntarily cooperating with law enforcement in implementing court-authorized interceptions. When it was established that Title III did not authorize a federal court to compel a telephone company to assist law enforcement, *Application of the United States For Relief*, 427 F.2d 639 (9th Cir. 1970), Congress promptly amended Title III to enable law enforcement to request the court approving the electronic surveillance to direct at the same time that the service provider provide all

[3] In 1986, the FCC responded to the request of law enforcement representatives and extended the period service providers had to retain toll records from six (6) to eighteen (18) months. *See* 47 CFR § 42.6.

information, facilities and technical assistance ("technical assistance") necessary to carry out the wiretap the court was authorizing. Since 1970, law enforcement has routinely included a request that the court direct the service provider to provide the essential technical assistance to make their electronic surveillance tools operational. When such an order is issued, it also directs law enforcement to reimburse the service provider for the costs it has incurred.

Nevertheless, service providers continued to resist assisting law enforcement in installing pen registers, which were not covered by Title III, but their efforts were unavailing. In *United States v. New York Telephone Co*., 434 U.S. 159 (1977), the Court held that a federal court could compel a telephone company to provide technical assistance (which the Court described as "meager," *id*. 434 U.S. at 175) to law enforcement in connection with the installation of a pen register. Service providers' arguments that they could not be compelled to provide technical assistance for traps and traces were similarly rejected. *See, e.g., In the Matter of the Application of the United States for an Order Authorizing Installation of a Pen Register or a Touch-Tone Decoder and a Terminating Trap*, 610 F.2d 1148 (3rd Cir. 1979).

These opinions emphasized that service providers have an interest in assisting law enforcement because they have a duty to see that their facilities are not used unlawfully. *See New York Tel. Co*., 434 U.S. at 174. The Court noted that private citizens, such as service providers, have a "duty to provide assistance to law enforcement officials when it is required." 434 U.S. at 176 n. 24. It has also been established by other courts that this duty to assist law enforcement can even include having the service provider itself execute a search warrant on behalf of law enforcement. *See, e.g., In the Matter of the Application*

of the United States for an Order Authorizing an In-Progress Trace of Wire Communications Over Telephone Facilities, 616 F.2d 1122 (9th Cir. 1980), *cited with approval* in *United States v. Bach*, 310 F.3d 1063 (8th Cir. 2002).

When Congress enacted the Foreign Intelligence Surveillance Act of 1978, (codified, as amended, at 50 U.S.C. §§ 1801 *et seq*.), and Pen Registers and Trap and Trace Devices, (codified as amended at 18 U.S.C. §§ 3121 *et* seq.)("Pen/Trap Statute"), (which was part of The Electronic Communications Privacy Act of 1986, Pub.L. 99-508, 100 Stat. 1848 ("ECPA")),[4] it ensured that law enforcement could compel a service provider to provide the technical assistance that is necessary to carry out the electronic surveillance authorized by the court. *See* 50 U.S.C. § 1805(b)(2)(B) and 18 U.S.C. §§ 3129(a) & (b) respectively. But until 1994 service providers incurred no significant expense or technical burden in complying with these court orders because they could use those facilities and services that were readily available in their networks to serve their customers to provide technical assistance to law enforcement.

With the enactment of CALEA, however, the nature, complexity and expense of the technical assistance that service providers are now compelled to provide changed radically. CALEA mandates that service providers deploy only those services that ensure that electronic surveillance remains a viable investigative tool for law enforcement. With

[4] ECPA set for the first time uniform procedures for providers of electronic communications services to produce a wide range of wire or electronic communications content, records, or other information to governmental entities. *See* Stored Wire and Electronic Communications and Transactional Records Access, codified as amended, at 18 U.S.C. § 2701 *et seq*. ("SCA"). The burdens on service providers created by SCA are significant. The USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001), increases this burden with, among other things, nationwide federal search warrants for email, federal search warrants for voice mail, and nationwide pen register and trap and trace orders in which the service provider may not even be named.

CALEA, service providers could no longer fulfill their obligation to provide technical assistance as they had in the past from service features that had been designed to serve their customers. The service provider's obligation changed from reactive to proactive, thereby making the provision of technical assistance a considerably more complex and expensive undertaking for service providers and forcing service providers to become more involved in the technical issues surrounding electronic surveillance. The expenditures incurred and technical complexities encountered by service providers to meet the obligations of CALEA, however, were considerably underestimated in 1994, and remain so today.

At the same time, service providers also risk criminal sanctions and civil liability if, in the course of providing their technical assistance, things go awry, *see*, *e.g.*, 18 U.S.C. §§ 2232 (d) and (e) and 18 U.S.C. § 2520, or they do not meet their CALEA obligations. 18 U.S.C. § 2522. Out of concern for these potential sanctions and liabilities, some service providers, particularly the large entities, have established sizable internal staffs to handle these matters. These service providers train and update their internal staffs on a continuing basis on both the technical and legal aspects of providing technical assistance.[5] With the variations between the federal and state electronic surveillance statutes, service providers face a complex challenge to ensure they are complying with valid court orders.[6] This challenge is even more complex for service providers that

[5] Service providers also face civil liability if they produce records to governmental entities improperly. 18 U.S.C. § 2707.

[6] With the increasing reliance on electronic records, service providers can be expected to conduct more of the complex searches authorized by courts on behalf of law enforcement. *See United States v. Bach*, 310 F.3d 1063 (8th Cir. 2002) and 18 U.S.C. § 2703(g). The task of complying with the appropriate process is becoming more

operate in multiple states because there are additional variances between state electronic surveillance statutes.

The financial reality for the service provider is that the production of customer records and the provisioning of technical assistance afford only a limited opportunity to recover its associated costs, making the production of records and the provision of technical assistance an increasingly expensive cost center. It is not surprising that many service providers, especially new entrants providing voice communications and traditional Internet service providers, have chosen to fulfill their obligations by looking to third parties for best-cost, efficient solutions associated with these support services rather than incur the burdensome expense. Many service providers have chosen Fiducianet to provide full end-to-end law enforcement support services.

III. INTRODUCING FIDUCIANET

Fiducianet is an agent of the service provider; Fiducianet describes itself as a "carrier agent."[7] It is not an independent contractor. The authority for a service provider to use an agent in matters of electronic surveillance is well established. Congress has long since recognized that service providers may use agents to carry out their technical assistance obligations. *See* Title III, 18 U.S.C. §§ 2511(2)(a)(ii) & 2518(4); Pen/Trap, 18 U.S.C. §§ 3124(a) & (b); and FISA, 50 U.S.C. § 1805, *as amended* by USA PATRIOT

---

challenging today. Compare *Fraser v. Nationwide Mutual Life Ins. Co*., 352 F.3d 107 (3d Cir. 2003) with *Theofel v. Farey-Jones*, 341 F.3d 978 (9th Cir. 2003), *petition of DOJ for rehearing denied*, 359 F.3d 1066 (9th Cir. 2004).

[7] Fiducianet has a wide range of client companies, including ISPs. For this reason, Fiducianet also describes itself as a "service provider agent" and/or "technical representative."

Act to add § 1805(h).[8] In the legislative history to CALEA, Congress said that court orders could be handled through individuals "authorized and designated by the telecommunications carrier." House Report No. 103-827, 5 USCCAN 3489, 3506, 103d Cong., 2d Sess. 1994 ("*House Report*").[9] As the Commission itself has recognized, providers may contract with a third party for its CALEA assistance needs in the same manner as the provider's contract for other network and operating support services. NPRM, ¶ 8 n. 11 (citations omitted).

In light of the fact that the legislative history to Title III sheds no light on what Congress intended, the concept of "agent" is defined by the common law. *See, e.g., Clackamas Gastroenterology Associates v. Wells,* 538 U.s. 440, 123 S.Ct. 1673 (2003); *Kolstad v. American Dental Ass'n*, 119 S.Ct. 2118, 2126 (1999). "Agency" under the common law is a consensual relationship in which one entity or person (Fiducianet) acts on behalf of another entity or person (the service provider) with the power to affect the legal rights and duties of the other person (the service provider). Restatement (Third) of Agency (2001), Tentative Draft No. 2, § 1.01, Comment *c*. Under an agency relationship, then, the service provider fulfills its statutory obligations through its agent, but as principal, it retains the ultimate responsibility to the courts and to law enforcement.

The services Fiducianet provides are governed by applicable laws and by the terms of the contract with the service provider. Although Fiducianet works cooperatively

---

[8] A service provider may also use an agent for services that are necessary to the rendition of service or to protect the rights or property of the service provider. Title III, 18 U.S.C. § 2511(2)(a)(i).

[9] Since this is much more expansive than the language in the statutory provision, this suggests that Congress did not intend to limit the capability to provide technical assistance only to service provider officers or employees.

with law enforcement to meet the terms of the court order, it is not an agent of law enforcement and is no more favorably inclined toward law enforcement than a service provider would be in the normal course of its business. In fact, Fiducianet's experience is that in many instances, especially for the small or rural service providers that have no experience in these areas, Fiducianet is more protective of the interests of the service provider and of the privacy rights of their customers than the service providers themselves tend to be.

The fees that customers pay for Fiducianet's services will vary according to the nature of the services the provider has contracted with Fiducianet to provide, but the amounts are very manageable when compared to the alternatives faced by service providers. There is no reason to believe that Fiducianet's fee structure encourages law enforcement to seek to conduct electronic surveillance.[10]

The service provider, as principal, controls what Fiducianet does through the detailed terms of its contract. To ensure that Fiducianet fulfills the service provider's obligations set out in the applicable electronic surveillance laws and in CALEA, Fiducianet indemnifies and holds the service provider harmless if Fiducianet acts outside the scope of its authority on behalf of the service provider.[11]

---

[10] Whether law enforcement is entitled to engage in electronic surveillance is a determination made exclusively by a court of appropriate jurisdiction. The amount law enforcement reimburses the service provider for the technical assistance provided is governed by the terms of the court order. Fiducianet s arranges for these reimbursements to be sent to its customers.

[11] As the agent of the service provider, Fiducianet is entitled under the electronic surveillance statutes to the same immunity and good faith defenses that protect the service provider.

In fact, third parties are no strangers to electronic surveillance operations. Law enforcement agents themselves are authorized to use third parties to play a significant role in electronic surveillance. Electronic surveillance may be conducted by an "individual operating under a contract with the Government, acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception." 18 U.S.C. §2518(5). If law enforcement can use non-government personnel to carry out the extremely sensitive task of the electronic surveillance itself, then it seems clear that a service provider can retain an agent to handle the less sensitive duty of providing the technical assistance for the court order.[12]

IV. HOW FIDUCIANET PROVIDES ITS SERVICES

It is important to provide more detail about Fiducianet's services, its investment in state-of-the-art technology, both hardware and software, and the expertise of its personnel.

Fiducianet offers service providers and manufacturers "innovative ways to meet the needs of the law enforcement community without adversely affecting the dynamic telecommunications industry." NPRM at ¶ 31. Most service providers want to support law enforcement's efforts to combat crime and terrorism in order to protect the public safety and our Nation's security. At the same time, however, service providers are in a very competitive marketplace where low cost providers have a market advantage.

[12] In matters involving telecommunications carriers' networks or records, the courts have for some time also allowed third parties to carry out critical portions of law enforcement's obligations. *See*, *e.g.*, *In the Matter of the Application of the United States for an Order Authorizing an In-Progress Trace of Wire Communications Over Telephone Facilities*, 616 F.2d 1122 (9th Cir. 1980) (involving the provisioning of technical assistance for a trap and trace), *cited with approval* in *United States v. Bach*, 310 F.3d 1063 (8th Cir. 2002) (involving the execution of a search warrant for electronic records).

Consequently, service providers, particularly new entrants, do not want to make the significant capital expenditures or incur the substantial overhead costs necessitated by these laws if there are alternatives available.

Fiducianet uses the deep domain knowledge and expertise of its personnel to design solutions that enable service providers to fulfill their obligations fully in a best-cost, efficient manner. Fiducianet personnel have over 60 years of combined experience in the telecommunications industry, law enforcement, and law enforcement support services, and they hold jointly with the telecommunications industry 9 patents related to technical assistance, including a pending patent for the "dial out" solution.

Fiducianet's significant investment in both hardware and software enables service providers to fulfill their lawful obligations and to be more competitive by allowing them to fulfill at lower costs the increasingly complex and expensive burdens imposed by CALEA as well as the federal and state electronic surveillance laws and by subpoenas, court orders or search warrants.

To develop its recommendation for a service provider, Fiducianet conducts a compliance assessment of the status of service provider's readiness under CALEA and the electronic surveillance laws by examining the service provider's network hardware and software and by collecting information about the service provider's electronic surveillance history.[13] Fiducianet then offers three (3) basic options to the service provider and recommends a best-cost solution for the service provider. None of Fiducianet's options involves an external system such as is described in the NPRM. Through its CALEA assessment, Fiducianet is able to make recommendations that

[13] Fiducianet also conducts compliance testing to assess the functionality of the service provider's capability under CALEA and other electronic surveillance laws.

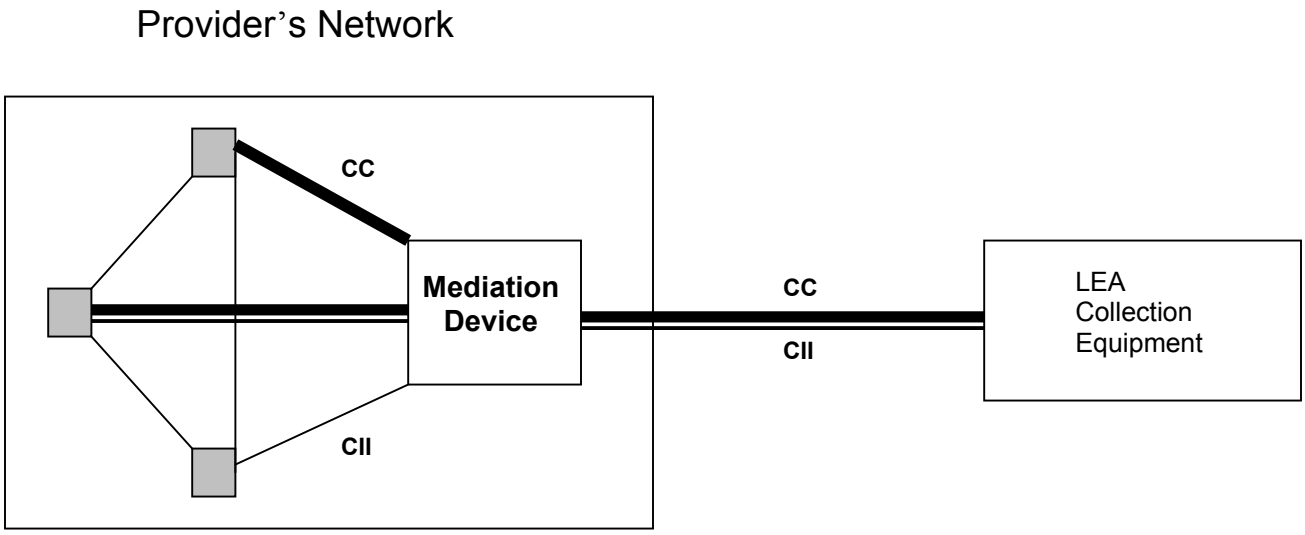
address actual, not theoretical concerns and that are scaled to the service provider's electronic surveillance experience.

Where the service provider has already made the investment in the technology required to comply with CALEA and other electronic surveillance laws, Fiducianet can maintain and utilize this technology, as a first option, on behalf of the service provider to provision the electronic surveillance and deliver the intercept directly to the law enforcement agency from the service provider's network. Where small or rural service providers have no electronic surveillance history, Fiducianet uses portable equipment, as a second option, that it can deploy in the service provider's network on a just-in-time basis.

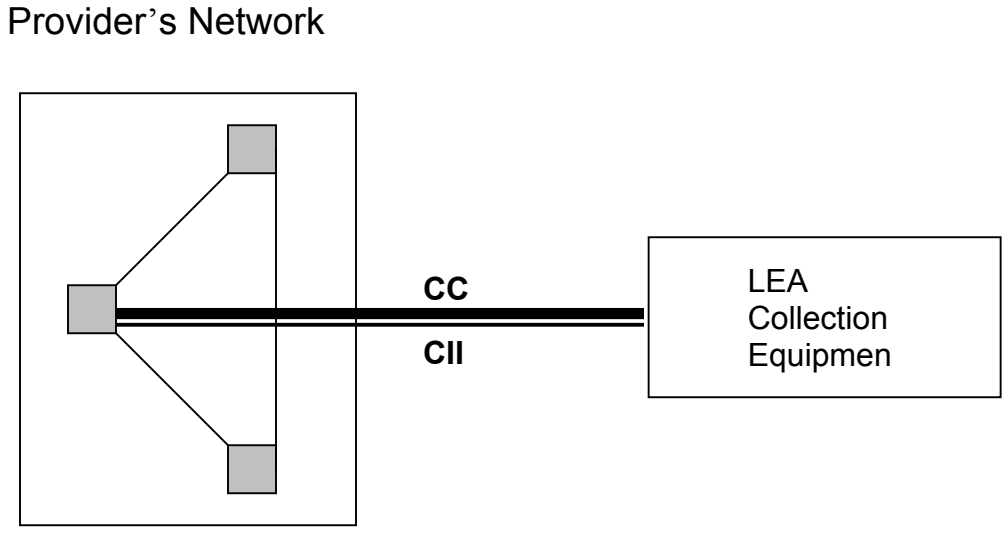
For other customers, Fiducianet configures solutions that involve installing equipment in the service provider's network. Fiducianet can then remotely activate this equipment through secure connections to the provisioning element in order to set up the technical assistance required by the court order.

In all cases, Fiducianet does not receive or monitor the information stream delivered to law enforcement. Fiducianet delivers the intercepted call-identifying information and/or call content directly from the service provider's network to the law enforcement collection/monitoring facility over circuits dedicated to fulfill the court order, which are paid for by the law enforcement agency.

Using the schematic format of Appendix C, here is a basic diagram of how Fiducianet provides technical assistance when mediation is required:



Using the schematic format of Appendix C, here is a basic diagram of how Fiducianet provides technical assistance when no mediation is required:



Neither option involves a network that is separate from the service provider's network. Rather, in Fiducianet's solutions the delivery function remains entirely within

the service provider's network and is similar to a solution that a service provider itself might deploy using its internal staffs to deliver call-identifying information and call content directly from the provider's network to law enforcement.

Under this option, Fiducianet offers the service provider an affordable and cost effective solution that has been scaled to the specific needs of the service provider and network growth.

There are other significant advantages to Fiducianet's solutions over an alternative that involves a network that is external to the provider's network. One such advantage is that if the parties agree, the service provider can assume responsibility for the operation of the equipment at some point in the future. This affords the service provider the opportunity to avail itself of Fiducianet's extensive domain knowledge and consulting expertise but at the same time it avoids the significant initial costs associated with obtaining and installing compliant technology as well as staffing and growing an internal infrastructure. A service provider would not have this option if it relied on an external system.

As these schematics demonstrate, Fiducianet provisions the equipment that has been placed in the service provider's network to intercept the content or access the call-identifying information authorized by the court order. Fiducianet then routes the intercepted content or accessed call-identifying information directly from the service provider's network to a point of presence where duly authorized law enforcement will be able to access and collect it. Fiducianet is able "to intercept to the exclusion of any other communications", CALEA § 103(a), so that the call content and/or call identifying information that is specified by the terms of the court order, and only that data, leaves the

provider's network. Additionally, Fiducianet remotely accesses the provider's network and provisions the switch for the electronic surveillance only when a valid court order has been served. Otherwise, there is no connection to the provider's network or external access to network elements.

In addition to the technical assistance itself, Fiducianet also handles many other obligations, such as receiving the court order on behalf of the service provider, ensuring that the order is valid and can be completed, coordinating with law enforcement, performing regular health and maintenance checks of the electronic surveillance equipment, and ensuring that throughout the period during which technical assistance is provided all the requirements of applicable CALEA System Security and Integrity policies and procedures are complied with, including the retention of the relevant documents in a secure facility and obtaining the affirmative intervention of a senior officer or employee of the service provider[14]

Fiducianet's solutions also fulfill the requirements of law enforcement as prescribed by CALEA Section 103. It expeditiously isolates and enables the court-ordered electronic surveillance; it excludes other communications that are not covered by the court order; and it delivers the specific content and/or call-identifying information directly from the service provider's network to a location or facility acceptable to the government and in a format that law enforcement can readily use. Moreover, Fiducianet's methods of delivering the content or call-identifying information directly from the service

[14] Fiducianet uses its own detailed System Security & Integrity Policies and Procedures, which are on file with the FCC. Fiducianet also serves as the custodian of this information and handles all liaison with law enforcement to ensure that the surveillance is conducted in accordance with the court order and that only the communications authorized to be intercepted are accessed and delivered to law enforcement.

provider's switch or network element to law enforcement involve no analysis or manipulation by Fiducianet. Consequently, its methods are not subject to the security risks to which an external solution may be exposed, and the content and/or call-identifying information sent directly out of the service provider's network is fully admissible in the courts in the same manner as information provided by the carrier using its own internal organization.

At the same time, Fiducianet's solutions address the interests of other parties impacted by CALEA. Fiducianet works with manufacturer(s) to develop solutions that make it easier for a manufacturer(s) to design systems that are cost-effective and reduce the likelihood that the manufacturer(s) will have to "force fit" features into equipment. NPRM, ¶ 71. For example, Fiducianet uses mediation devices developed with the cooperation of several manufacturers and mediation systems vendors to deliver the content or call-identifying information directly to law enforcement in formats that law enforcement can readily use.

V. FIDUCIANET'S CONCERN FOR PRIVACY

The NPRM seeks comments on how a telecommunications carrier that relies on a trusted third party would meet its obligations under § 103(a) to protect the privacy and security of call content and call identifying-information that are not subject to interception as well as to protect the information about the electronic surveillance itself. NPRM, ¶ 76.

Customer privacy is a bedrock principle of CALEA as well as the electronic surveillance laws, and as an agent of the service provider it is one of Fiducianet's core

concerns. Fiducianet's has developed solutions that protect the privacy and security of the service provider's customers whose content and call-identifying information are not subject to the court order. These solutions involve strict compliance with the applicable statutes, with the terms of the court order themselves, with applicable regulations, and with the terms of the contract between the service provider and Fiducianet. It is in the vital interests of Fiducianet, therefore, that it fulfills its responsibilities correctly the first time; it does not expect to be given a second chance.

Congress has enacted a strict statutory scheme that imposes significant criminal sanctions and civil liability for violations of electronic surveillance laws. Title III, 18 U.S.C. § 2511(2)(a)(ii), imposes civil liability for disclosing the existence of any interception, any surveillance or the device used to accomplish the interception or surveillance. The Pen/Trap Statute, 18 U.S.C. § 3123(d), seals the court order and directs the service provider not to disclose the existence of the pen register or trap and trace. 18 U.S.C. §§ 2232(d) & (e) make it a felony to obstruct or impede an interception by notifying or attempting to notify any person that an application has been made to the court or that the court has approved an interception. There are also state counterparts for these federal statutes. These statutes serve as substantial constraints on Fiducianet to maintain the privacy and security of the electronic surveillance just as they constrain the service providers themselves.

The court orders that authorize electronic surveillance direct service providers [15] not to disclose the existence of the court order, the electronic surveillance, or the

[15] The court orders for technical assistance name the service provider and hold it accountable to fulfill the courts' directives whether it uses its own employees or agents such as Fiducianet.

investigation unless and until ordered by the court. Any entity served with a court order containing such a non-disclosure provision, therefore, could be held in contempt of court for violating its terms. Such a potential sanction serves as another substantial constraint on Fiducianet as well as the service provider to maintain the privacy and security of the electronic surveillance.

Fiducianet's contracts contain covenants that Fiducianet will meet all the requirements of applicable laws and regulations as well as the service provider's policies and procedures. Fiducianet carefully selects its personnel and conducts background and credit checks before hiring them. Service providers can audit the records Fiducianet maintains on behalf of the service provider to satisfy themselves that Fiducianet is complying with the terms of the contract and with applicable law and regulations.

Applicable regulations include the CALEA System Security and Integrity regulations ("SS&I") found at 47 CFR Part 64, §§ 64.2101-2106. Fiducianet reviews each service provider's statement of its SS&I policies and procedures. Where appropriate, Fiducianet files a revised statement with the Commission that fully complies with the regulatory requirements. Included in these SS&I policies and procedures is the requirement that Fiducianet will report to the appropriate law enforcement agency any act of compromise of the electronic surveillance to unauthorized persons. 47 CFR § 64.2103(c). Furthermore, no electronic surveillance is activated unless and until Fiducianet has the affirmative authorization from a senior officer or employee as required by CALEA § 105 and applicable regulations.

Fiducianet's procedures serve the privacy interests of the service provider's customers as well as law enforcement. Fiducianet does not have access to the call content

or call-identifying information in that it is delivered directly from the service provider's network element or switch to law enforcement. Fiducianet does not analyze or manipulate the call-identifying information in any manner. The data that leaves the service provider's network is the data specified by the court order and only that call-identifying information is delivered to law enforcement. Fiducianet remotely accesses the intercept provisioning equipment, mediation equipment, or CALEA compliant network element deployed in the service provider's network and provisions the technical assistance only upon the service of a valid court order. Fiducianet does not directly access a service provider's customers' communications.

In summary, many service providers choose Fiducianet's services because they are confident that Fiducianet understands the privacy concerns involved in providing technical assistance and that Fiducianet takes all necessary steps to protect the privacy interests of all interested parties.

VI. COMMENTS ON QUESTIONS RAISED IN APPENDIX C

The NPRM seeks comments on five (5) questions propounded in Appendix C.

What is the feasibility of having the network equipment deliver all packets of a subject to an External System?

There are at least two concerns with delivering all packets to an external system. First, there is a question of reliability. As the packets move from point to point during the transmission, there is an increased risk of degradation or failure. Additionally, the number of court orders that involve only call-identifying information (Pen Registers and/or Trap and Trace Devices) far exceeds the number of orders for call content (full interception) or both full content and call-identifying information. Under the new

CALEA Packet Cable I04 specification, "mediation" device(s) will be responsible for decoding the post cut-through digits or "Dialed Digit Extraction." This means that in order to provide law enforcement with post cut-through digits, the switch must instruct the cable modem termination system to forward a copy of the voice packets transmitted by the target (i.e., outgoing calls) as well as the communication content received by the target (i.e., incoming calls) to the mediation device(s). The mediation device(s) then separates the content from the call-identifying information and sends only the latter to law enforcement. Sending all of the packets, as the question suggests, to a system that is not part of the service provider's network means that even where the court order authorizes law enforcement to receive only call-identifying information the service provider's network will be delivering both content and call-identifying information to the external system for mediation that is outside the service provider's network and is not subject to its control. The risks inherent in this external system do not exist under Fiducianet's options.

In cases where the subject has a dynamically assigned IP address, is it still feasible for network equipment to deliver all of the subject's packets to an External System?

Using Fiducianet's model, it is immaterial. For an external system, it is technically possible. However, by delivering all of the subject's packets to an external system, the network or service provider faces an undue burden because there is more interaction with other networks elements besides the switch as well as higher bandwidth requirements. There is also a greater risk of breaching the customer's privacy.

Are there cases where surveillance of a subject with a dynamic IP address could be better accomplished with a Mediation Device, instead of an External

System; or with a direct link between network equipment and LEA collection equipment?

Other than the increased cost associated with higher guaranteed bandwidth, it is irrelevant to Fiducianet. Use of an external system creates an issue of scalability and the risk of transmission errors and lost data where the number of simultaneous technical assistance orders is high. Complete coverage may require multiple installations of probes. A mediated solution would work the same as a direct link, but there may be significant privacy issues.

Could the packets be provided by one or more probes or "sniffers" on a line into a router or switch, instead of the router or switch itself?

Reminiscent of the technical challenges that prompted CALEA in 1994, a sniffer can only capture the packets that it has access to. With the advanced calling features available in the switching network today, many situations arise in which the content flow will not be visible to the sniffers in the network. Since the network element that is responsible for switching the call is the only element that "knows" all of the information pertaining to the call, the information must be obtained from that network element, not exclusively from sniffers.

Could a subject's packets be provided to the External System by devices operating at layers below the Internet Protocol layer? For example, could a subject's packets be provided by an ATM switch based on virtual circuit identifiers, or by a cable modem termination system based on a MAC address?

The amount of data that needs to be processed increases by a significant magnitude when going below the application layer. The amount of processing required to process raw packets to reconstitute or reconstruct the elements of service used by the

target can lead to results that are inconsistent with the switch, creating questions about the integrity of the call content or call-identifying information.

VII. WHETHER THERE IS A "TENSION" BETWEEN RELYING ON A TRUSTED THIRD PARTY AND RELYING ON "SAFE HARBOR" STANDARDS

The NPRM suggests that there may be some "tension" between relying on a trusted third party and relying on the "safe harbor" standards of CALEA. Fiducianet does not see any tension with respect to its services.

The scheme established by Section 107 of CALEA "defers, in the first instance, to industry standards organizations" *House Report*, 5 USCCAN at 3506, by allowing for the adoption of an industry standard for compliance. A service provider deploying electronic surveillance equipment that conforms to the industry-adopted capability standards is deemed compliant with Sections 103 and 107 of CALEA. If the same equipment is deployed in the service provider's network by the trusted third party, the service provider enjoys the same level of compliance.

Fiducianet works closely with the service provider's equipment manufacturer and with third party vendors of electronic surveillance support equipment (sniffers, mediation platform providers, and others) but does not itself design or deploy proprietary equipment into the service provider's network for provisioning of electronic surveillance, for mediation, or for delivery of intercepted call-identifying information or call content. Solutions deployed by Fiducianet are the same solutions developed in the normal course of business based on industry standards or otherwise considered compliant by the

manufacturers selling electronic surveillance or network monitoring equipment to the service providers in today's marketplace.

The NPRM recognizes, however, that compliance with a "safe harbor" standard is not required by CALEA. ¶ 77. CALEA's legislative history provides that "compliance with the industry standards is voluntary, not compulsory. Carriers can adopt other solutions for complying with the capability requirements . . . ." *House Report*, 5 USCCAN at 3507. The NPRM reinforces this by stating that "individual carriers are free to choose any technical solution that meets the assistance capability requirements of CALEA, whether based on an industry standard or not." NPRM ¶ 12. The NPRM, then, gives service providers the option of using the publicly available technical standard, NPRM ¶ 98, or using "CALEA-compliant equipment." NPRM ¶ 99. So long as the solution meets the requirements of § 103, law enforcement has no basis to complain because CALEA does not guarantee "one-stop shopping" for law enforcement. *Id*. at 3502.

In summary, since Fiducianet's solutions use commercially available equipment, Fiducianet does not see any "tension" as the NPRM suggests may exist.

VIII. COMMENTS ON QUESTIONS RAISED BY TIA

The NPRM seeks comments on several questions raised by the Telecommunications Industry Association ("TIA"), NPRM ¶ 74.

Would it be adequate to require network equipment to provide only packet content under the terms of J-STD-025-A, and to allow the manufacturers of that equipment to assume that any additional analysis of the content will be provided by an external system?

J-STD-025-A applies to circuit-switched call-identifying information; it has nothing to do with packet or content. For pure packet, J-STD-025-B applies and PacketCable I04 has been adopted for the packet cable environment. Whatever standards are developed by the industry groups to deliver call content and call-identifying information should be followed. It would be acceptable to further analyze data through a system that is external to the switch but internal to the service provider's network.

May a particular network equipment supplier conclude that its customers can find other CALEA solutions from other suppliers, and at that point withdraw from the CALEA process without liability?

This question appears to be directed to manufacturers who have specific and significant responsibilities under CALEA. Because Fiducianet uses commercially available industry solutions, however, a network equipment supplier could not draw this conclusion with respect to Fiducianet. If appropriate, Fiducianet may submit reply comments addressed to the views on this question expressed by other interested parties.

Could a supplier be forced to reenter the CALEA market if the third-party suppliers it was counting on go out of business?

It is unclear what presumptions have been made in propounding this question and who the third party is in this question. A supplier may create a solution to fulfill its obligations to its client under CALEA that uses only the supplier's internal resources, or it may create a solution that uses a subcontractor, or third-party supplier.

In the normal course of business, however, telephone equipment manufacturers and other supplies may cease doing business in the United States, such as Mitel and Alcatel, or go out of business altogether. For this reason, when service providers select

their manufacturers carefully, they factor into their selection process whether the manufacturer or the subcontractors chosen by the manufacturer are viable and stable.

If "third-party suppliers" is intended to refer to Fiducianet, service providers select agents, such as Fiducianet, using the same factors as they use for their selection of providers of other products or services. In the unlikely event that Fiducianet would go out of business, however, there would be no significant impact on its service providers and no significant break in meeting their CALEA capabilities. Because the equipment that Fiducianet uses resides in the service provider's network, the service provider could assume operational responsibilities for providing technical assistance just by adding staff. A service provider would not have this option using an external system if the third-party supplier should choose to withdraw from the CALEA service market for business reasons.

What impact would reliance on a trusted third party have on developing standards for CALEA compliance?

Insofar as Fiducianet's services are concerned, there would be little or no impact. The industry standards-setting organizations develop standards that ensure compatibility with numerous vendors' products and services. Fiducianet relies on the commercially available equipment solutions just as the service providers themselves do. Since Fiducianet provides its services in the same manner as the service provider would if it were handling the responsibility itself to provide technical assistance with its internal resources, service providers are not disadvantaged in fulfilling their CALEA responsibilities by using Fiducianet. This would probably not be true for an external system.

What tools would a service bureau need to interface with various products from numerous vendors and would this responsibility be difficult to meet or too expensive?

What tools a service provider would have to use would depend on the published standards. It is immaterial that a service bureau like Fiducianet is involved. As new products are introduced or new companies are established, the standards and equipment may have to be modified. Designing any modification would be the responsibility of the equipment manufacturer and the fact that a third party is involved would not shift this burden nor, by itself, make designing the medication more difficult. As to relative costs, however, it is not as complex or expensive when the mediation equipment is deployed within the service provider's network.

Are there incentives to keep manufacturers engaged in developing CALEA compliance solutions if carriers relied on a trusted third party?

The statutory obligations of CALEA should serve as sufficient incentive to manufacturers. Implementation of the industry-adopted standards is an integral part of developing a technical solution for CALEA. Manufacturers, therefore, have to stay involved in the standards development process. Section 106 of CALEA.

IX. WHAT FINANCIAL MODEL, IF ANY, SHOULD FUNDING A TRUSTED THIRD PARTY TAKE?

NRPM suggests that it may be appropriate to develop a means to fund a trusted third party, and provides three (3) alternatives: the trusted third party could be owned by the packet service provider; or owned by law enforcement; or owned by an independent

surveillance service provider who contracts with individual carriers. Although the NPRM does not request comments, Fiducianet submits its comments on this matter.

Fiducianet does not see any need for a special arrangement for funding a trusted third party. The nominal fees for Fiducianet's services are well within the financial ability of even small or rural service providers.

Creating an independent surveillance service provider creates another level of bureaucracy, creates more complexity, clouds the issues of responsibility, and potentially interferes with the service providers' ability to control CALEA costs.[16]

Fiducianet believes that there may be significant privacy and legal concerns if law enforcement funded, paid for, and/or operated a trusted third party. As law enforcement agencies' comments have already pointed out, however, their financial resources are already exhausted or stretched to the limit. Funding for a trusted third party would require budget approvals at the federal and state levels.

X. DOES THE AVAILABILITY OF A TRUSTED THIRD PARTY APPROACH MAKE CALL-IDENTIFYING INFORMATION "REASONABLY" AVAILABLE TO A TELECOMMUNICATIONS CARRIER UNDER SECTION 103(a)(2)?

Because the NPRM uses the broader term "telecommunications carrier," Fiducianet assumes this includes both circuit-mode and packet-mode service providers. Based on our experience, we agree with the NPRM that the availability of a firm such as Fiducianet makes call-identifying information "reasonably" available through the application of a commercially available industry solution.

[16] Creating an independent surveillance service provider may require amending electronic surveillance statutes.

XI. WHAT ARE THE APPROXIMATE RELATIVE COSTS OF INTERNAL SYSTEMS VERSUS EXTERNAL SYSTEMS FOR PACKET EXTRACTION?

Based on the comments that service providers have provided to Fiducianet, our solutions are very cost effective when compared to all of the costs required to create and support "internal systems" with a department of full-time employees. We have no direct knowledge of the fees that other trusted third parties charge their customers, but we do know that the fees we charge law enforcement for technical assistance are well below the amounts charged by many service providers who maintain their own internal system with full-time employees.

CONCLUSION

Service providers engage Fiducianet as their agent because they can fulfill their obligations under CALEA and the electronic surveillance laws in an efficient and cost effective manner. Because Fiducianet provides a scalable mirror image of the services that a service provider would be expected to use if its internal staff was doing the work itself, there is no adverse impact on law enforcement requirements. As Fiducianet has demonstrated, the services provided by Fiducianet are in the interests of service providers, the privacy of their customers, and law enforcement.

H. Michael Warren
President
Fiducianet
mike.warren@fiducianet.biz

Douglass J. McCollum
General Counsel, VP Services
Fiducianet
doug.mccollum@fiducianet.biz

2121 Cooperative Way, Suite 200
Herndon, VA 20171
Tel: 703-796-1100
Fax: 703-689-0566